Procédure de mise à niveau de FireAMP Private Cloud 3.0.1

Contenu

Introduction

Ce document décrit comment mettre à niveau un cloud privé FireAMP (vPC) version 2.4.4 vers version 3.0.1. Notez que la procédure de mise à niveau nécessite une nouvelle instance de machine virtuelle pour la version 3.0.1.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Installation d'un modèle Open Virtual Appliance (OVA) dans VMWare ESXi
- Connaissances de base sur le fonctionnement et le fonctionnement du cloud AMP virtuel

Configuration matérielle requise

Voici la configuration matérielle minimale requise pour le cloud privé FireAMP :

- vSphere ESX 5 ou supérieur

- 8 processeurs
- 64 Go de RAM
- 1 To d'espace disque libre sur le data store VMWare
- Type de lecteur : SSD requis
- Type RAID : Un groupe RAID 10 (répartition des miroirs)
- Taille minimale du magasin de données VMware : 1 To
- Lectures aléatoires minimales du magasin de données pour le groupe RAID 10 (4K) : 60 000 E/S PAR seconde
- Écritures aléatoires de magasin de données minimum pour le groupe RAID 10 (4K) : 30 000 E/S PAR seconde

> **Attention** : Le cloud privé OVA crée les partitions de disque, il n'est donc pas nécessaire de les spécifier dans VMWare.

> **Note**: Reportez-vous au Guide d'utilisation du cloud privé FireAMP pour plus d'informations sur les exigences matérielles.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cloud privé FireAMP 2.4.4
- Cloud privé FireAMP 3.0.1
- VMWare ESXi 5.0 ou supérieur

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Processus de mise à niveau

Cette section fournit des instructions pas à pas sur la façon de collecter la sauvegarde à partir de la version 2.4.4 du cloud privé FireAMP et de la restaurer correctement sur la version 3.0.1 du cloud privé FireAMP.

> **Attention** : Le processus de mise à niveau peut introduire un temps d'arrêt dans votre environnement. Les connecteurs (y compris AMP for Networks connectés à votre cloud privé virtuel) qui utilisent le cloud privé peuvent perdre la connectivité au cloud virtuel et peuvent avoir des fonctionnalités défectueuses à cause de cela.

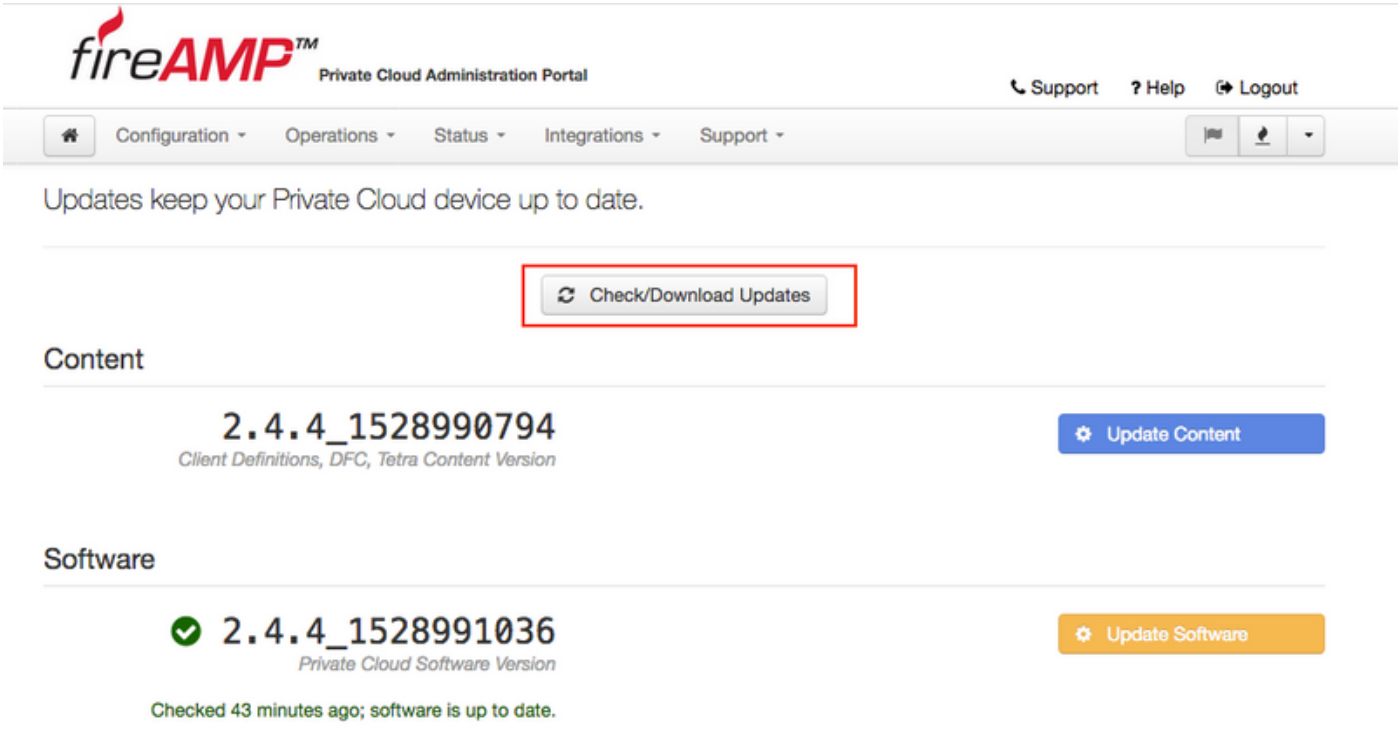
1. Mise à jour du téléchargement et de l'installation

Assurez-vous que votre cloud privé virtuel FireAMP 2.4.4 est à jour.

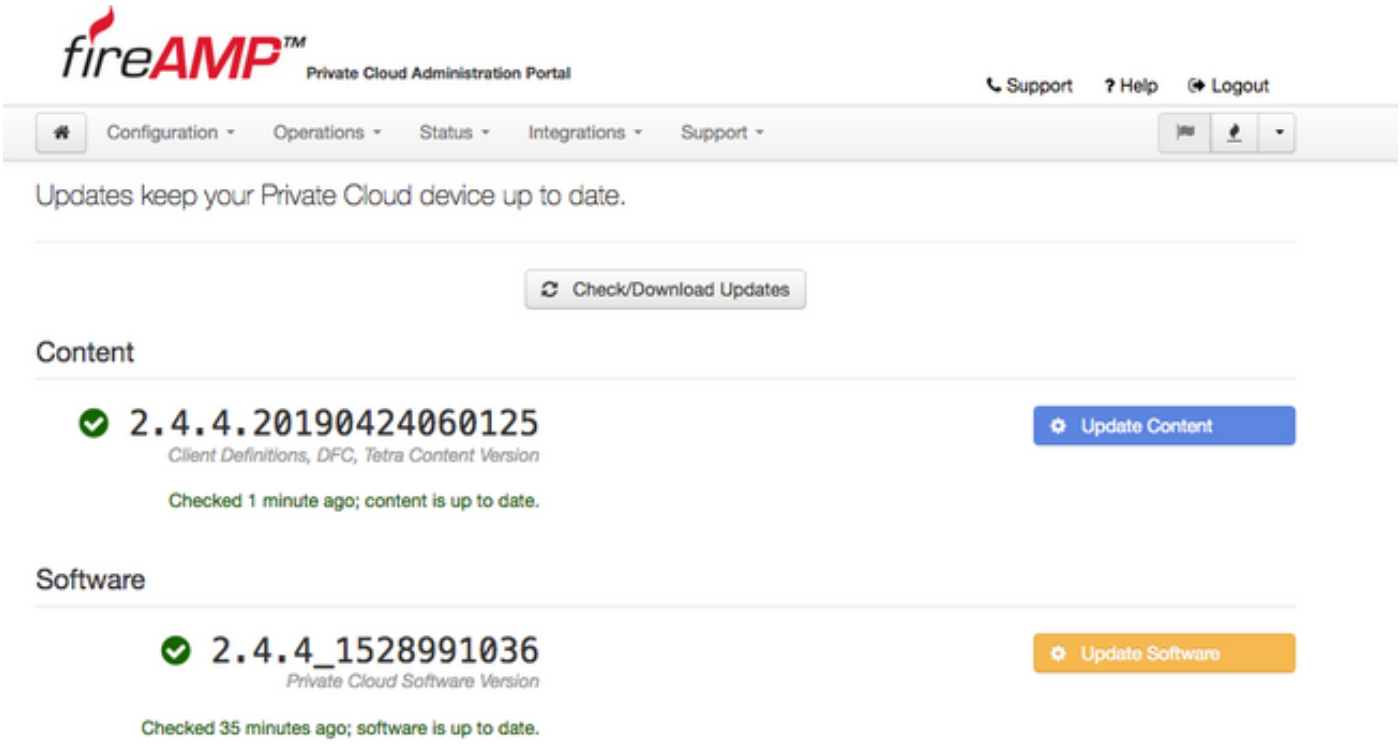
Étape 1. Accédez à **Operations** -> **Update Device** dans Administrator Portal.

Étape 2. Cliquez sur le bouton **Vérifier/Télécharger les mises à jour**, comme illustré dans l'image,

pour vous assurer que votre cloud privé virtuel FireAMP, d'où provient la collecte de sauvegarde, est à jour (au niveau du contenu et des logiciels).



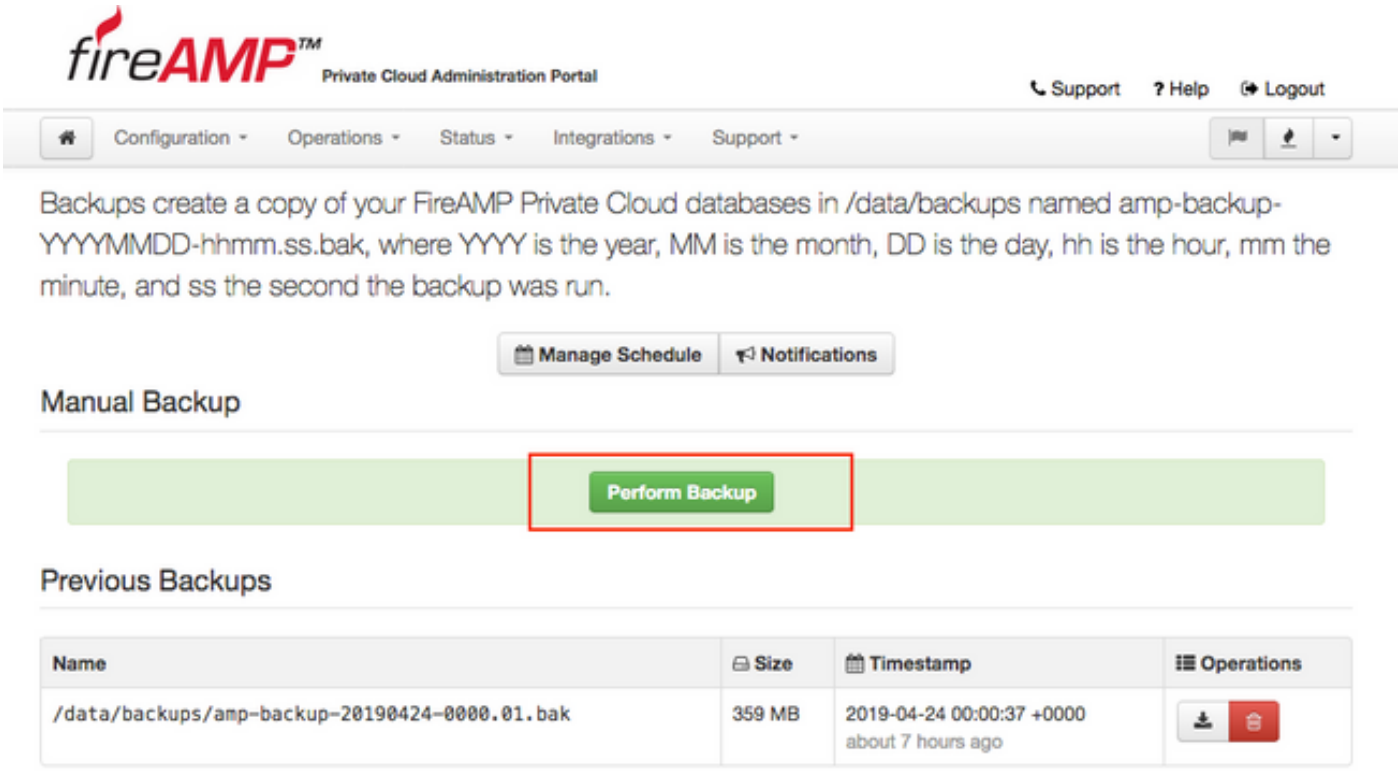
Étape 3. Une fois les mises à jour de contenu et de logiciel installées, la page de mise à jour affiche les informations indiquant que le périphérique est à jour, comme l'illustre l'image.



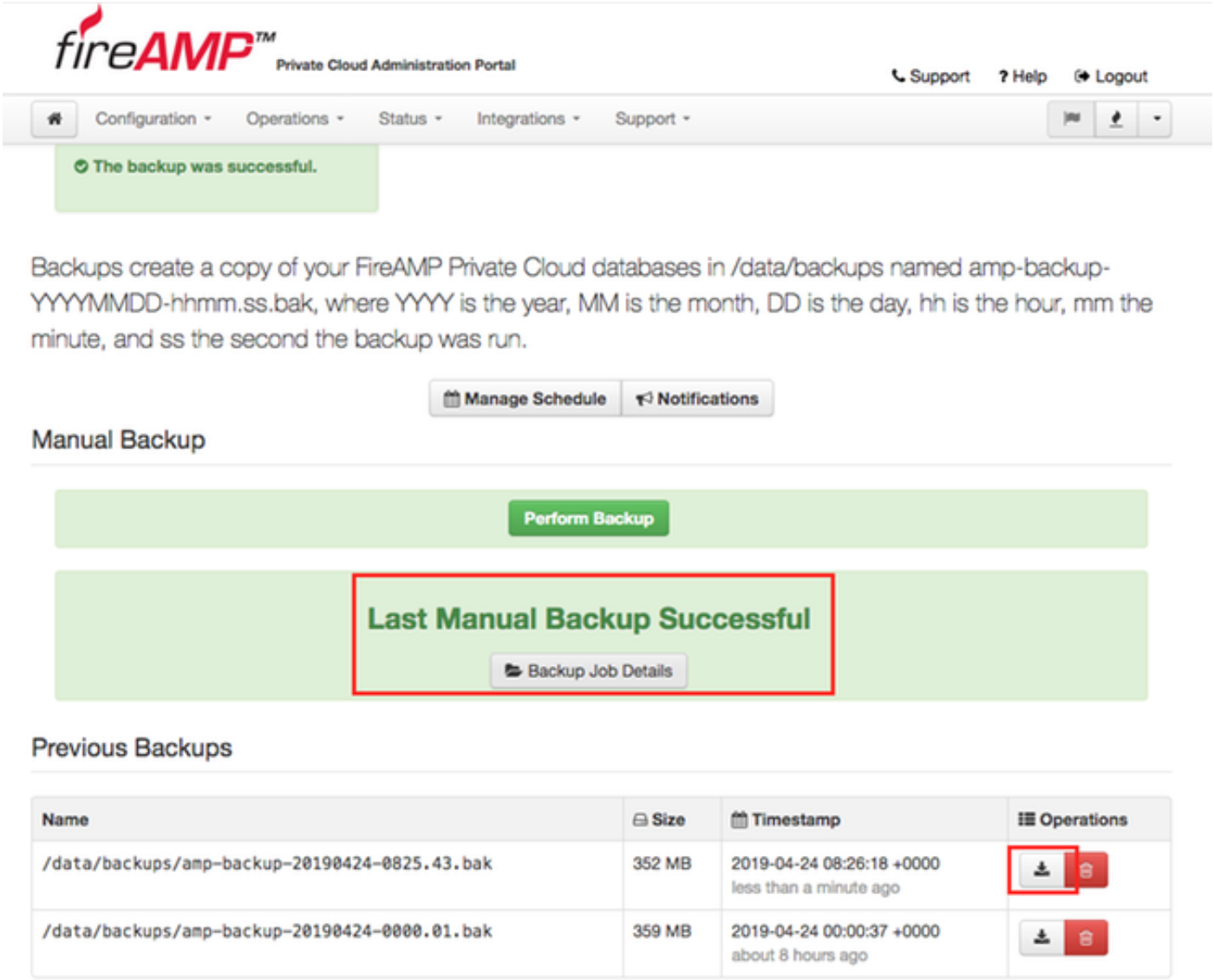
2. Collecte et arrêt de sauvegarde

Étape 1. Accédez à **Opérations -> Sauvegardes.**

Étape 2. Dans la section Manual Backup (Sauvegarde manuelle), cliquez sur le bouton **Perform Backup (Exécuter la sauvegarde)**. La procédure démarre une création de sauvegarde.



Étape 3. Une fois le processus terminé, la notification réussie apparaît, comme l'illustre l'image.



Étape 4. Cliquez sur bouton. Assurez-vous que la sauvegarde est correctement téléchargée et enregistrée dans un emplacement sûr.

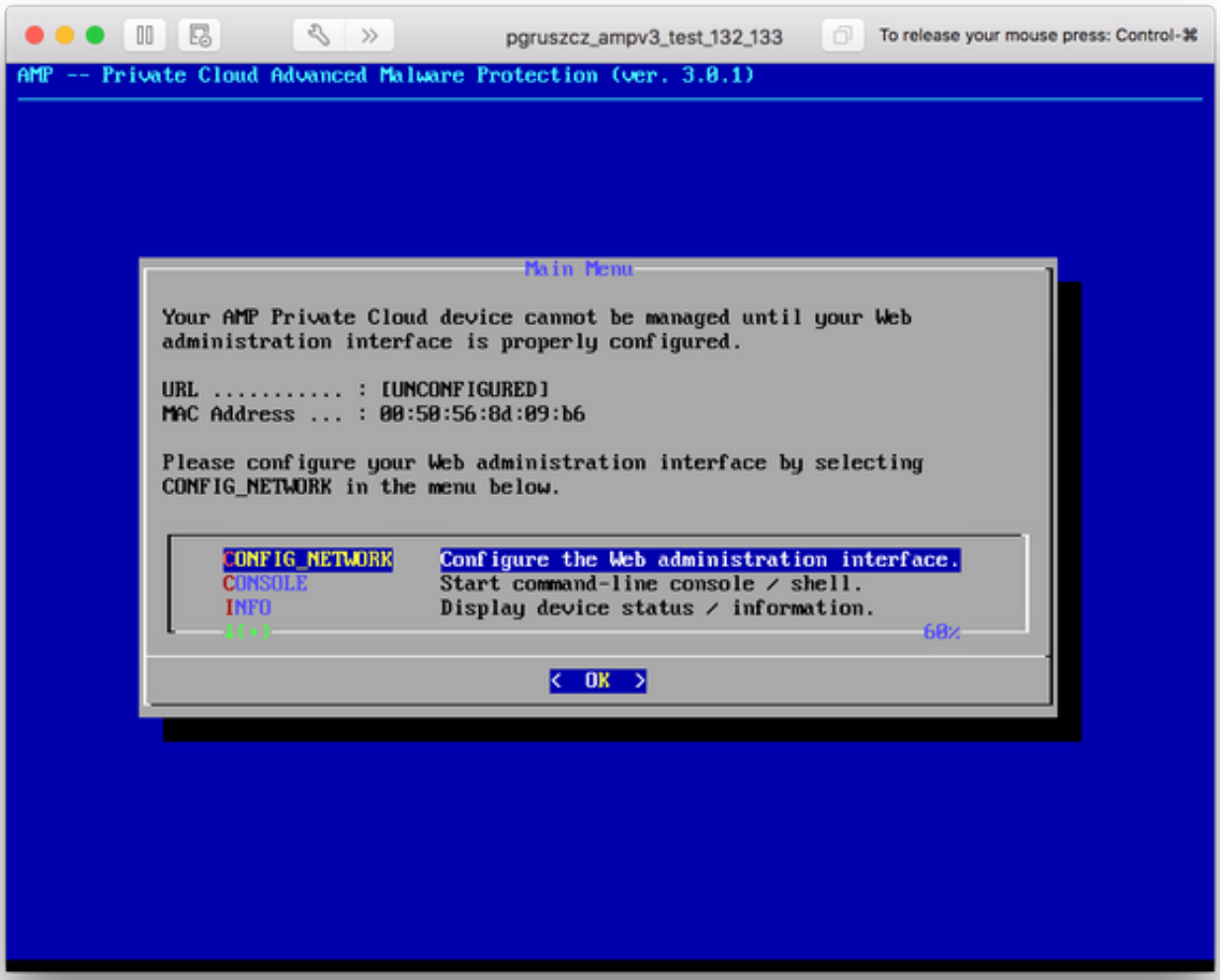
3. Nouvelle installation de version

Cette section suppose que Virtual Machine pour 3.0.1 FireAMP Virtual Private Cloud est déjà déployé. La procédure d'installation relative à Virtual Machine pour 3.0.1 OVA sur VMWare ESXi se trouve sous la liaison : Déployer un fichier OVA sur un serveur ESX.

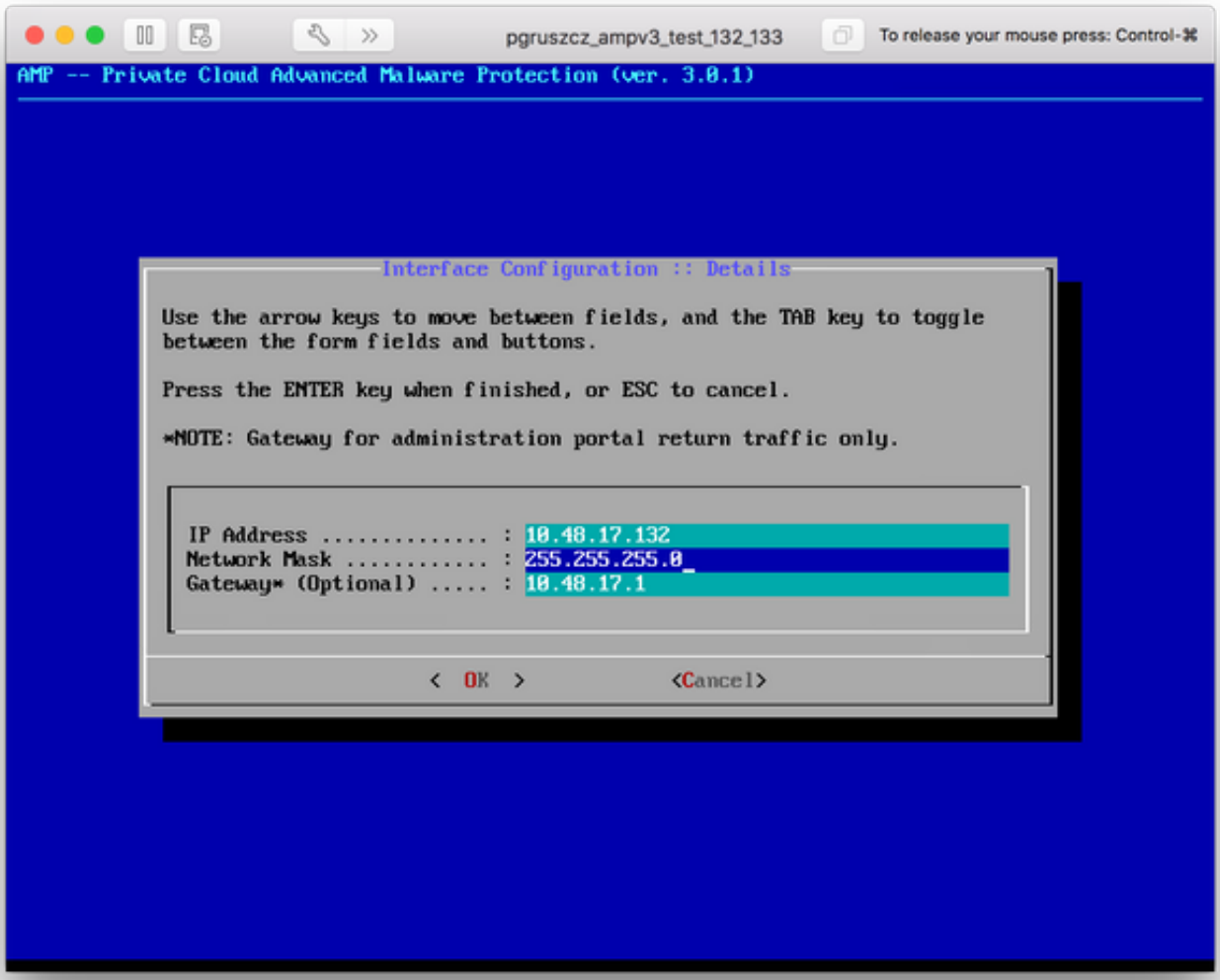
> **Note**: La procédure présentée dans cet article utilise exactement les mêmes noms d'hôte et adresses IP pour FireAMP Virtual Private Cloud 2.4.4 et 3.0.1. Lorsque vous suivez ce guide, vous devez arrêter FireAMP Virtual Private Cloud 2.4.4 après la collecte de la sauvegarde.

Étape 1. Ouvrez le terminal de console pour l'instance de machine virtuelle nouvellement créée avec la version 3.0.1 installée. Vous pouvez naviguer à travers les touches **Tab**, **Enter** et **flèches**.

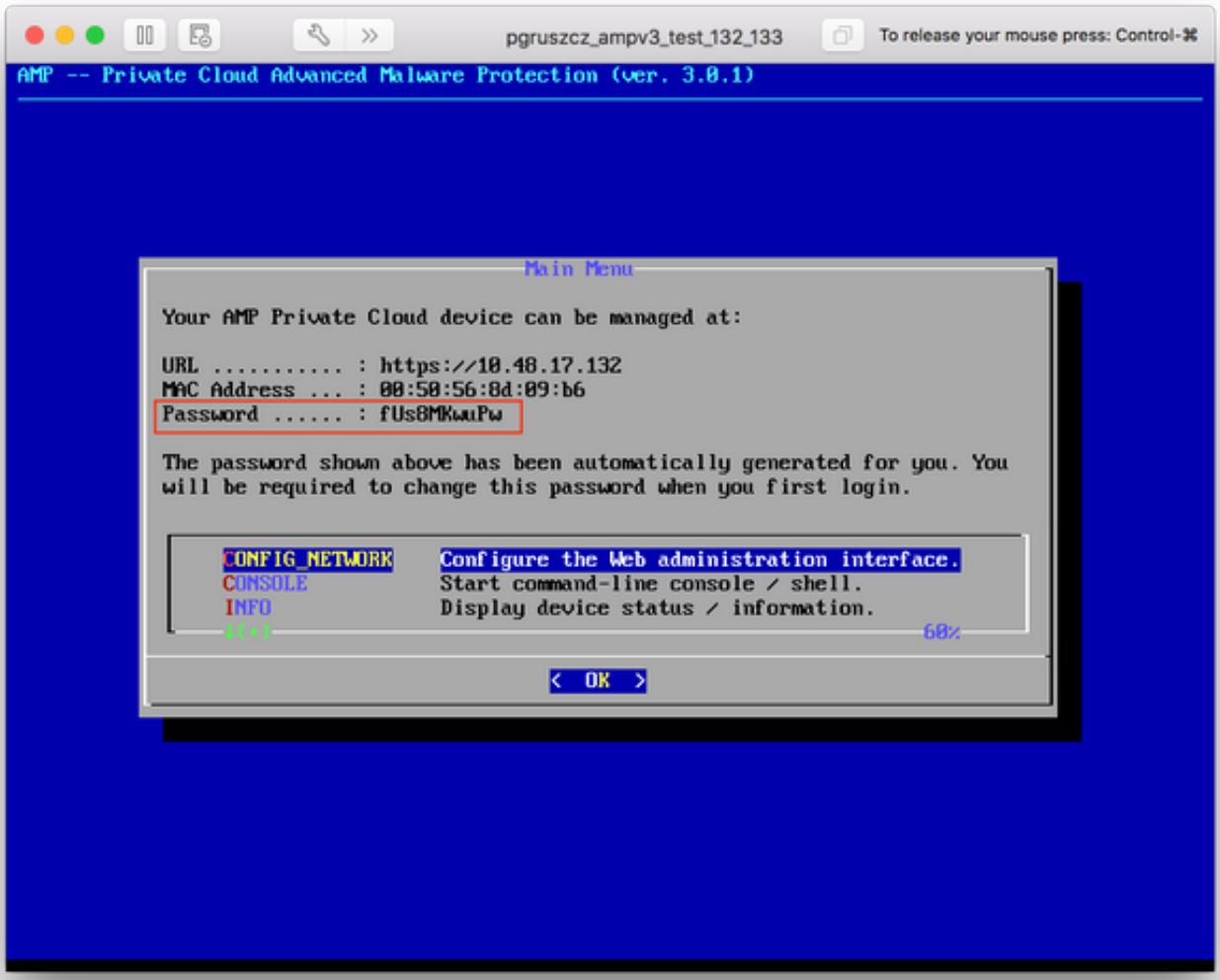
Étape 2. Accédez à **CONFIG_NETWORK** et cliquez sur la touche **Entrée** de votre clavier pour commencer la configuration de l'adresse IP de gestion du cloud privé FireAMP. Si vous ne voulez pas utiliser DHCP, sélectionnez **Non** et appuyez sur **Entrée**.



Étape 3. Entrez l'**adresse IP**, le **masque réseau** et la **passerelle par défaut**. Accédez à **OK**, comme l'illustre l'image. Appuyez sur la touche **Entrée**.

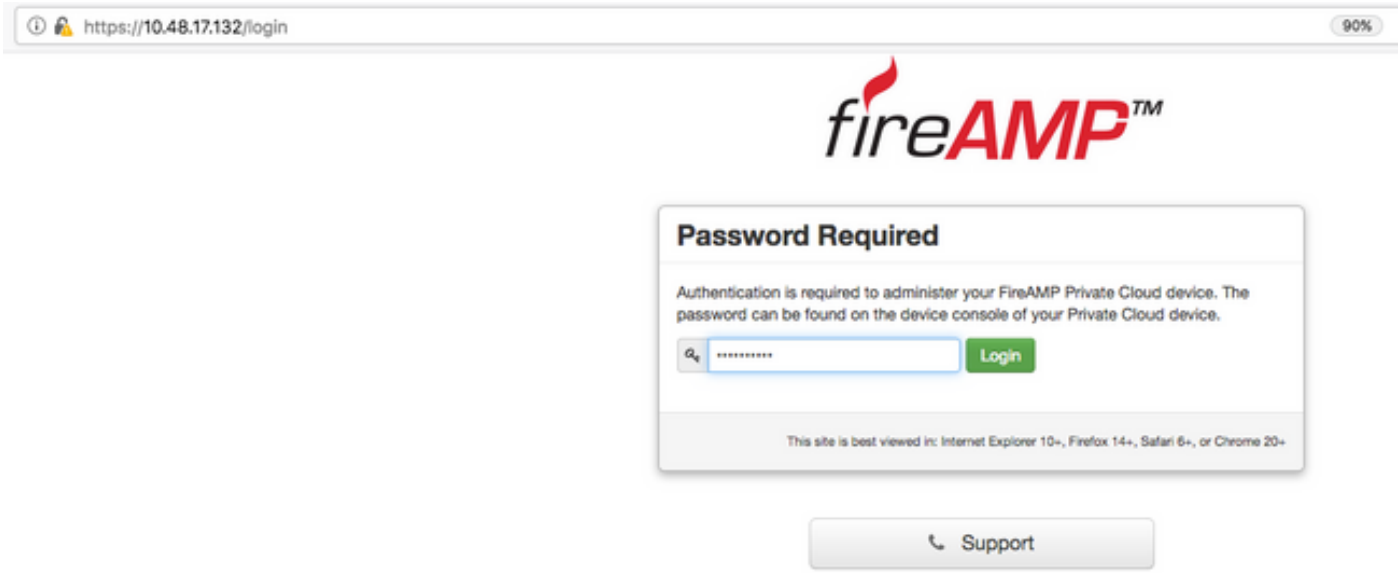


Étape 4. La modification de la configuration du réseau nécessite un redémarrage de l'interface. Après le redémarrage, le menu principal de la console réapparaît, comme l'illustre l'image. Cette fois, une adresse IP apparaît sur la ligne d'URL. Notez également que le **mot de passe** initial s'affiche. Il s'agit d'un mot de passe unique (plus tard appelé **mot de passe initial**) utilisé dans la configuration Web.

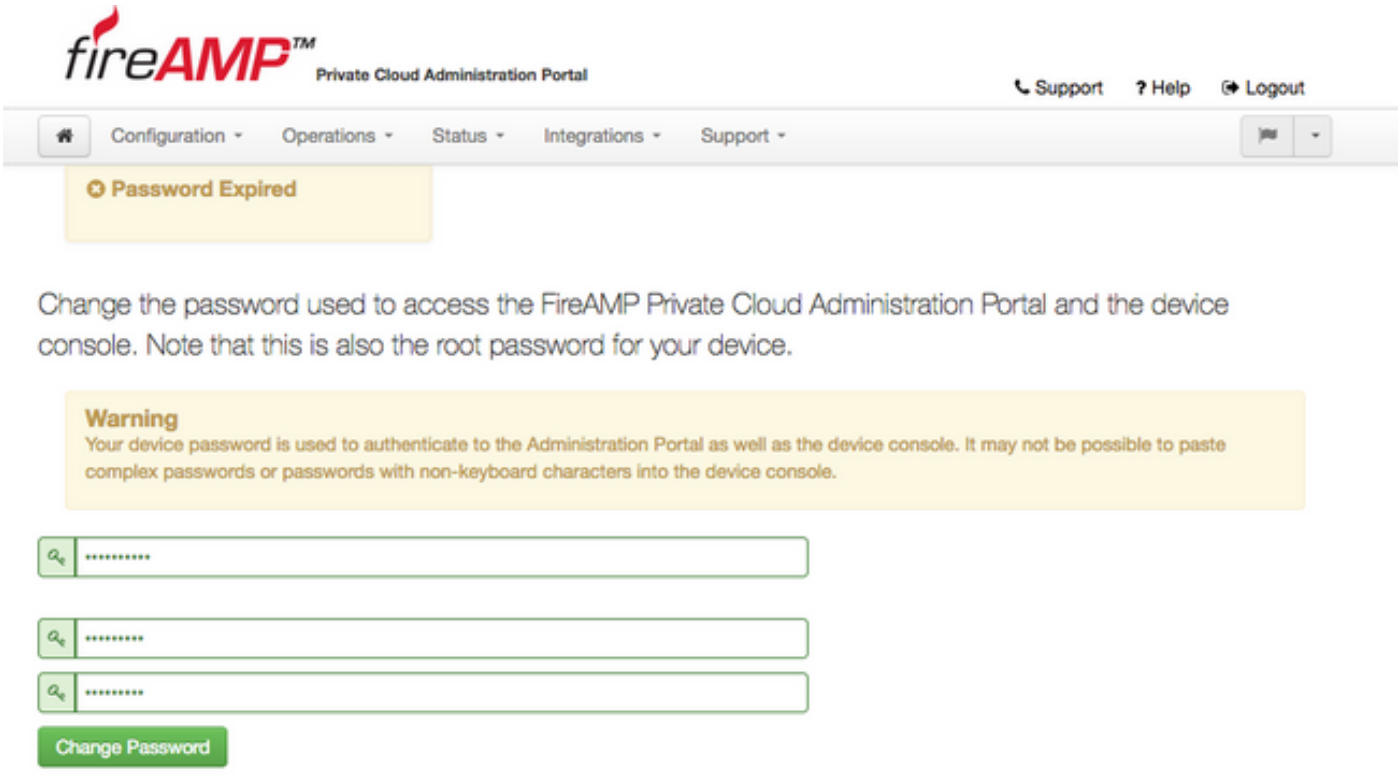


Étape 5. Ouvrez un navigateur Web et accédez à l'adresse IP de gestion de l'appliance. Vous recevez une erreur de certificat car le cloud privé FireAMP génère initialement son propre certificat HTTPS. Configurez votre navigateur pour qu'il fasse temporairement confiance au certificat auto-signé du cloud privé FireAMP.

Étape 6. Vous obtenez un écran pour saisir un mot de passe, comme le montre l'image. Utilisez le **mot de passe initial** de la console. Cliquez sur **Connexion**.

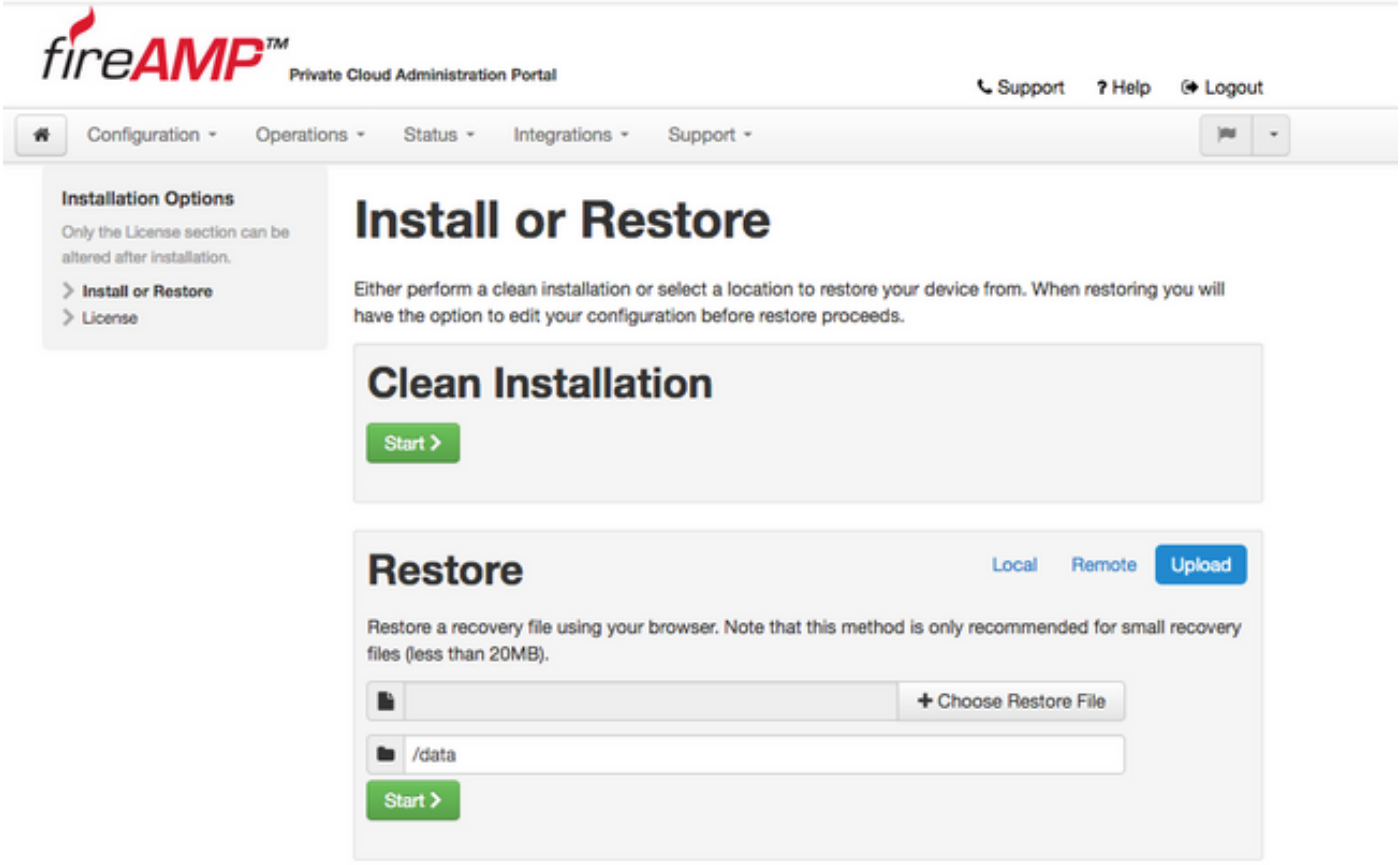


Étape 7. Après une connexion réussie, vous devez modifier le mot de passe. Utilisez le **mot de passe initial** de la console dans le champ **Ancien mot de passe**. Utilisez votre nouveau mot de passe deux fois dans les champs **Nouveau mot de passe**. Cliquez sur **Modifier le mot de passe**.



4. Restauration de sauvegarde

Étape 1. La page d'accueil du portail Admin présente deux méthodes d'installation de FireAMP Virtual Cloud 3.0.1, comme l'illustre l'image.



Étape 2. Vous pouvez choisir l'une des trois méthodes suivantes pour télécharger le fichier de sauvegarde vers l'instance de cloud privé virtuel FireAMP nouvellement créée :

Local - Restaure la configuration à partir d'un fichier de sauvegarde déjà présenté sur le périphérique (vous devez placer le fichier sur l'appliance via SFTP ou SCP). Les fichiers sont extraits dans le répertoire approprié une fois que le processus de restauration commence. Pour cette raison, recommandé est /data directory.

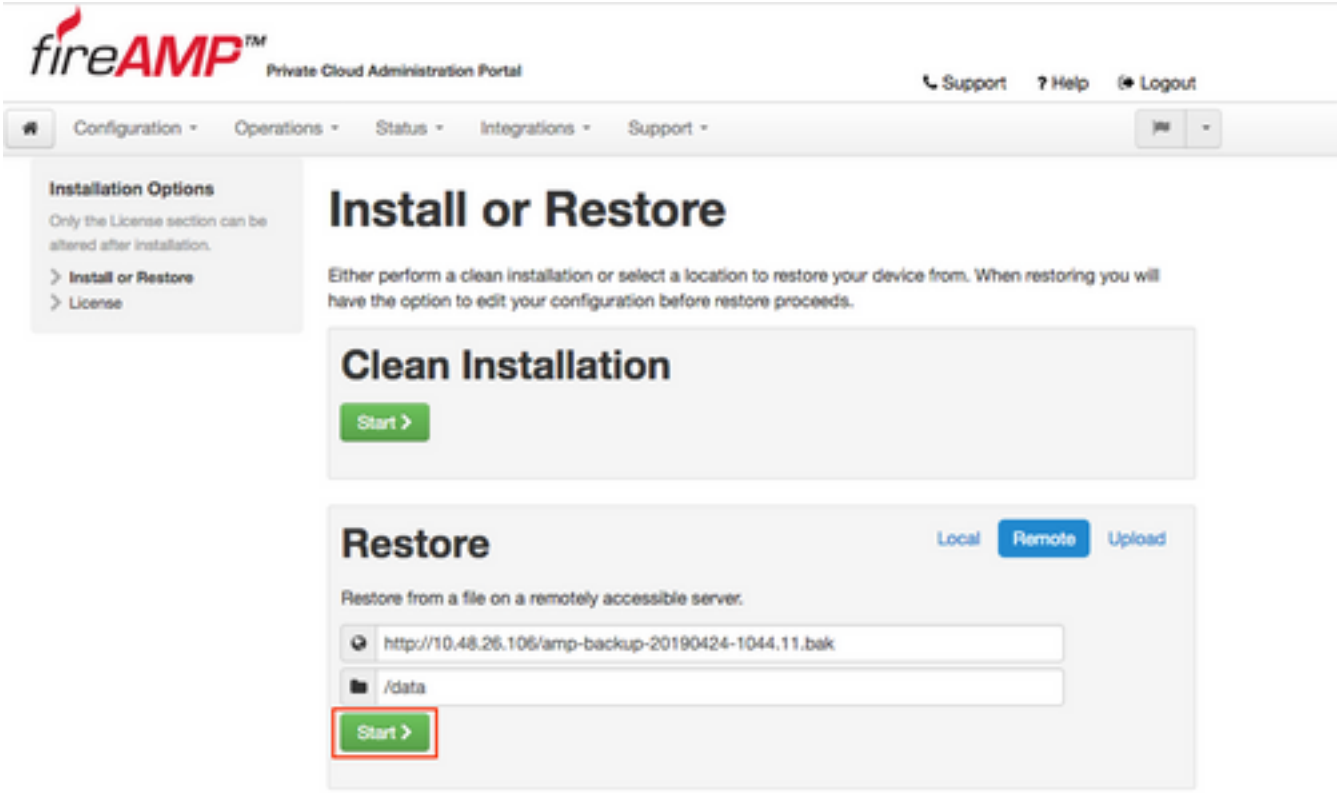
Distant : restauration à partir d'un fichier sur un serveur HTTP accessible à distance.

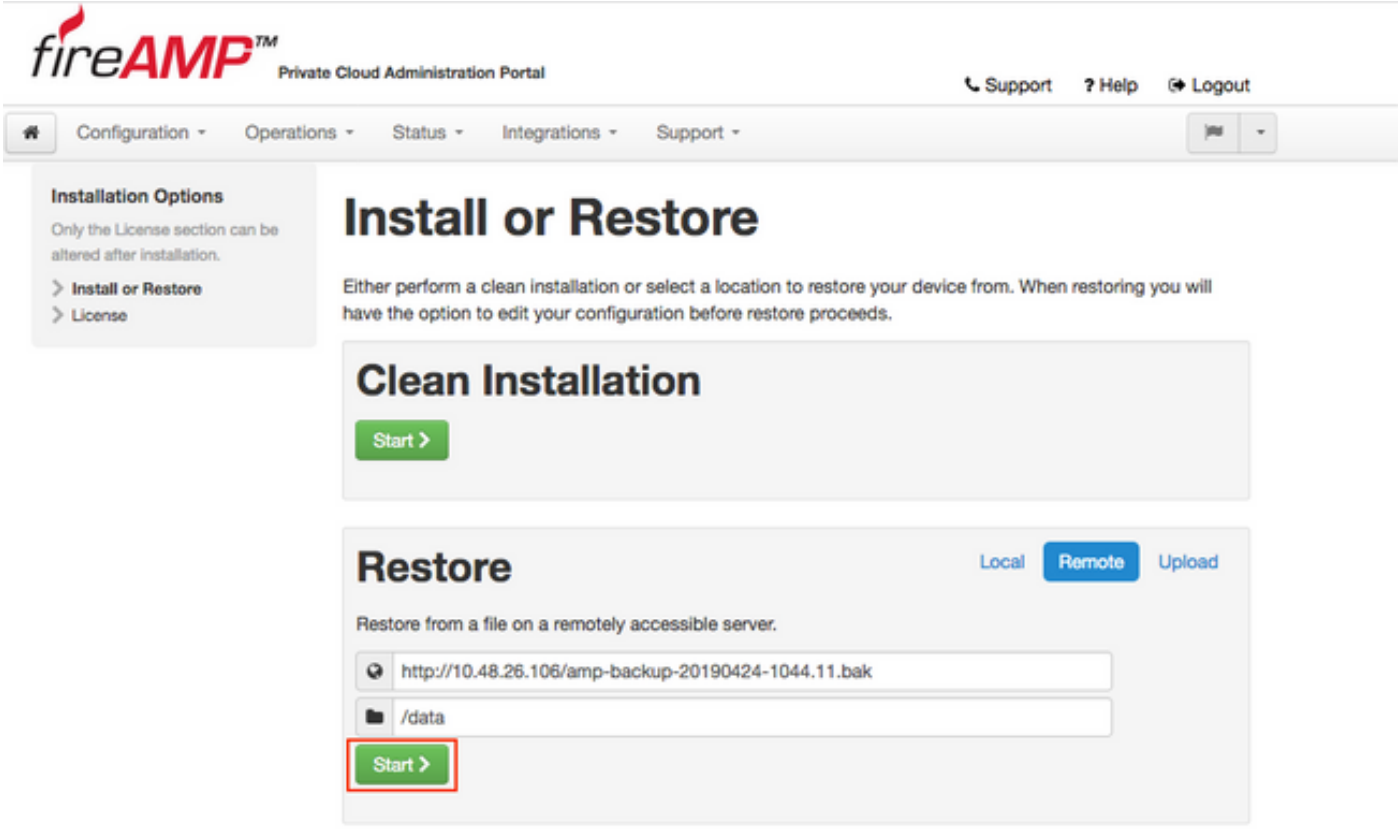
Upload - Restaurer à partir du fichier téléchargé par votre navigateur. Fonctionne uniquement si votre fichier de sauvegarde est inférieur à 20 Mo.

Dans cet exemple, l'option distante a été choisie.

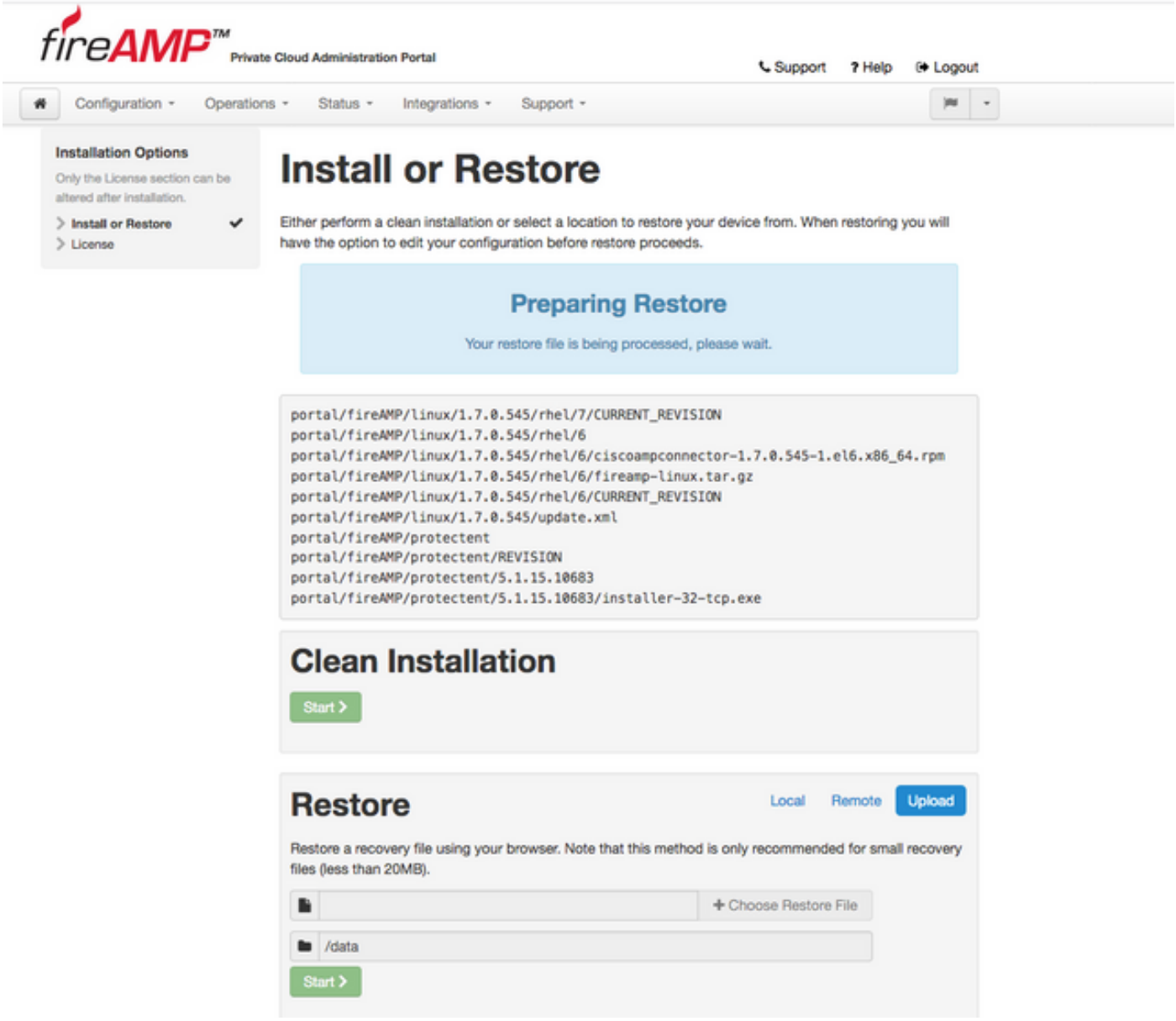
> **Note**: Une connectivité appropriée doit être autorisée pour le serveur HTTP. Le fichier de sauvegarde doit être accessible du point de vue du cloud privé.

Cliquez sur le bouton **Démarrer** pour poursuivre la restauration, comme illustré dans l'image.

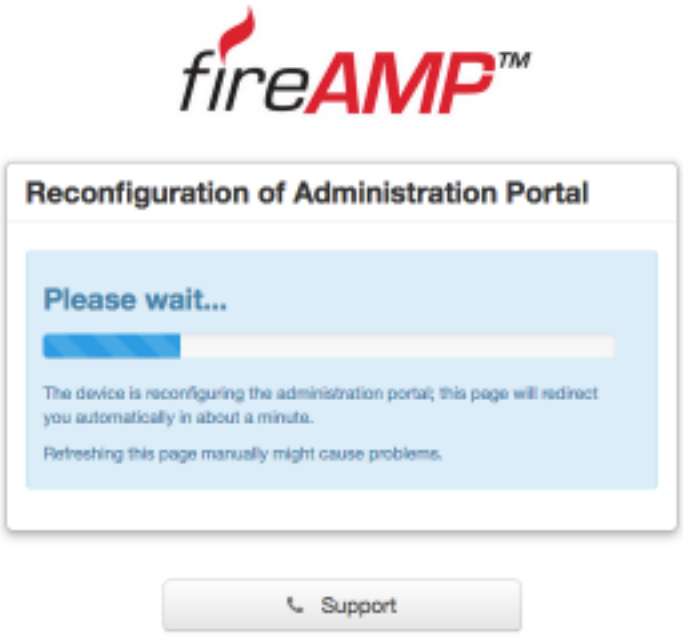




Étape 3. La procédure de restauration à partir d'une sauvegarde remplace votre configuration actuelle. Les clés d'hôte SSH de votre périphérique et le mot de passe du portail d'administration sont remplacés. Vous pouvez consulter certaines parties de votre configuration en ce qui concerne l'installation.

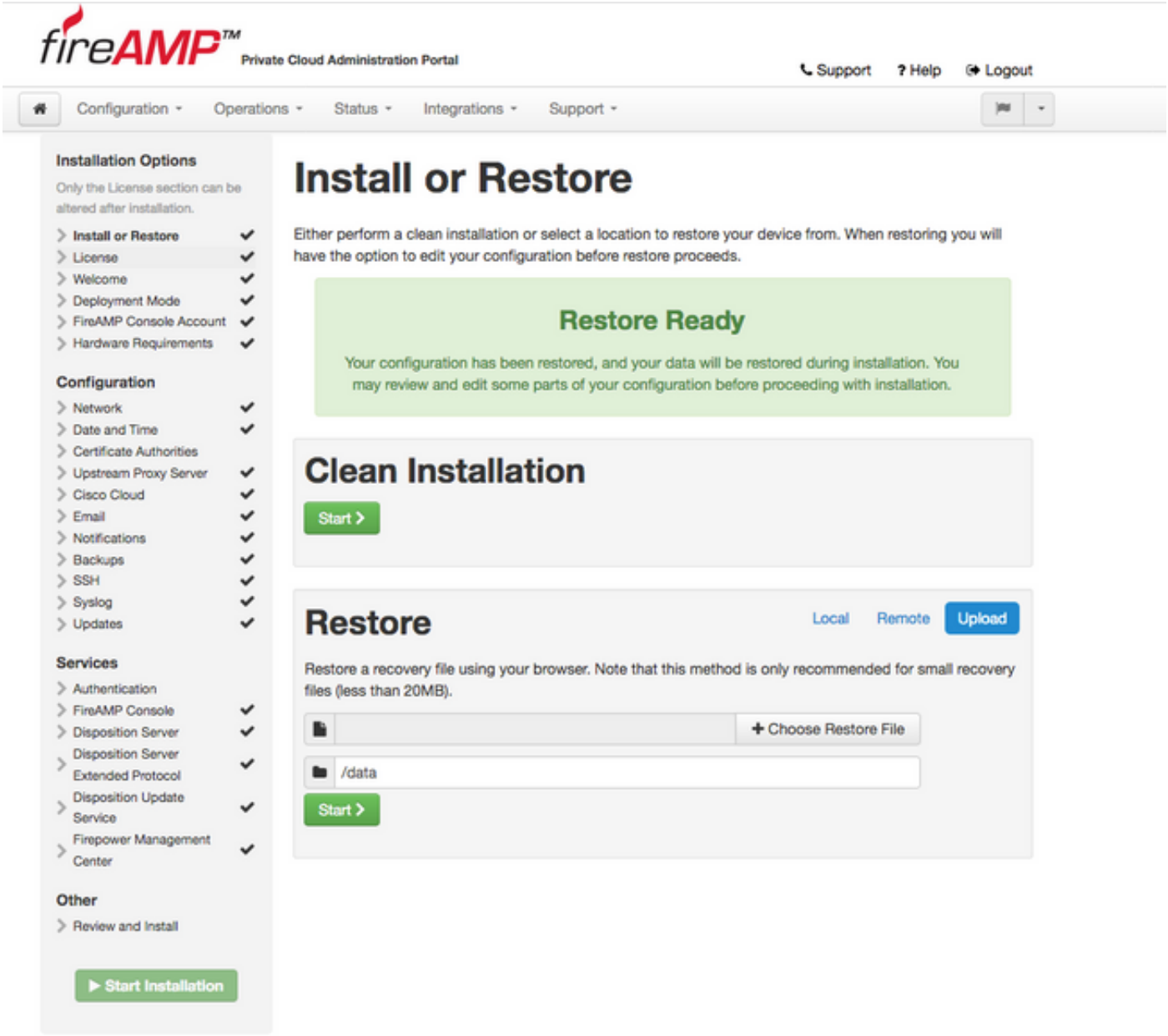


Étape 4. Après une copie réussie du fichier de sauvegarde, la page de restauration présente un message contextuel comme indiqué sur l'image. Cliquez sur le bouton **Reconfigurer le portail d'administration maintenant** pour terminer la procédure de restauration.



Étape 5. Une fois la reconfiguration terminée, la page du portail Administration s'affiche à nouveau, comme l'illustre l'image. À partir de maintenant, pour vous connecter, vous devez utiliser le mot de passe de la sauvegarde de cloud privé virtuel FireAMP 2.4.4.

L'image montre la plupart du travail pour l'installation correcte comme déjà fait (coches). Elle est attendue car la sauvegarde restaure la configuration à partir de FireAMP Virtual Private Cloud 2.4.4.



5. Autorités de certification

La version 3.0.1 de FireAMP Virtual Private Cloud introduit de nouvelles fonctionnalités et de nouveaux comportements en termes de fonctionnement du système. Vous devez les configurer et les terminer avant de commencer l'installation.

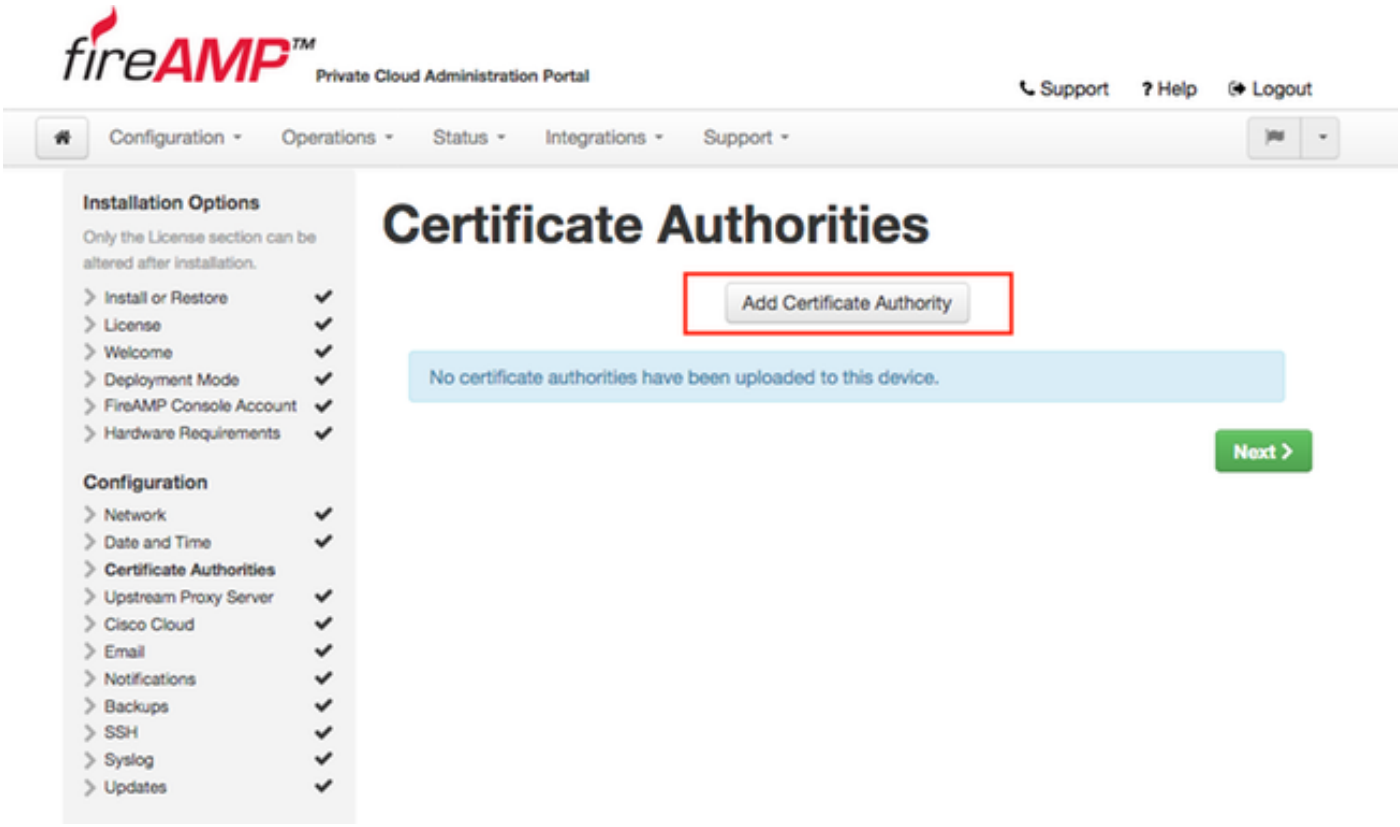
Le premier élément qui est nouveau et qui n'était pas présent dans la version précédente est **les autorités de certification**.

La page **Autorités de certificat** vous permet de gérer les certificats racine de vos services si vous voulez utiliser une autorité de certificat personnalisée. Vous pouvez télécharger ou supprimer votre certificat racine si nécessaire.

> **Note**: Le magasin approuvé des autorités de certification est utilisé uniquement pour les services de cloud virtuel (pour créer et valider la chaîne de certificats appropriée). Il n'est pas utilisé pour diverses intégrations vPC, comme ThreatGrid.

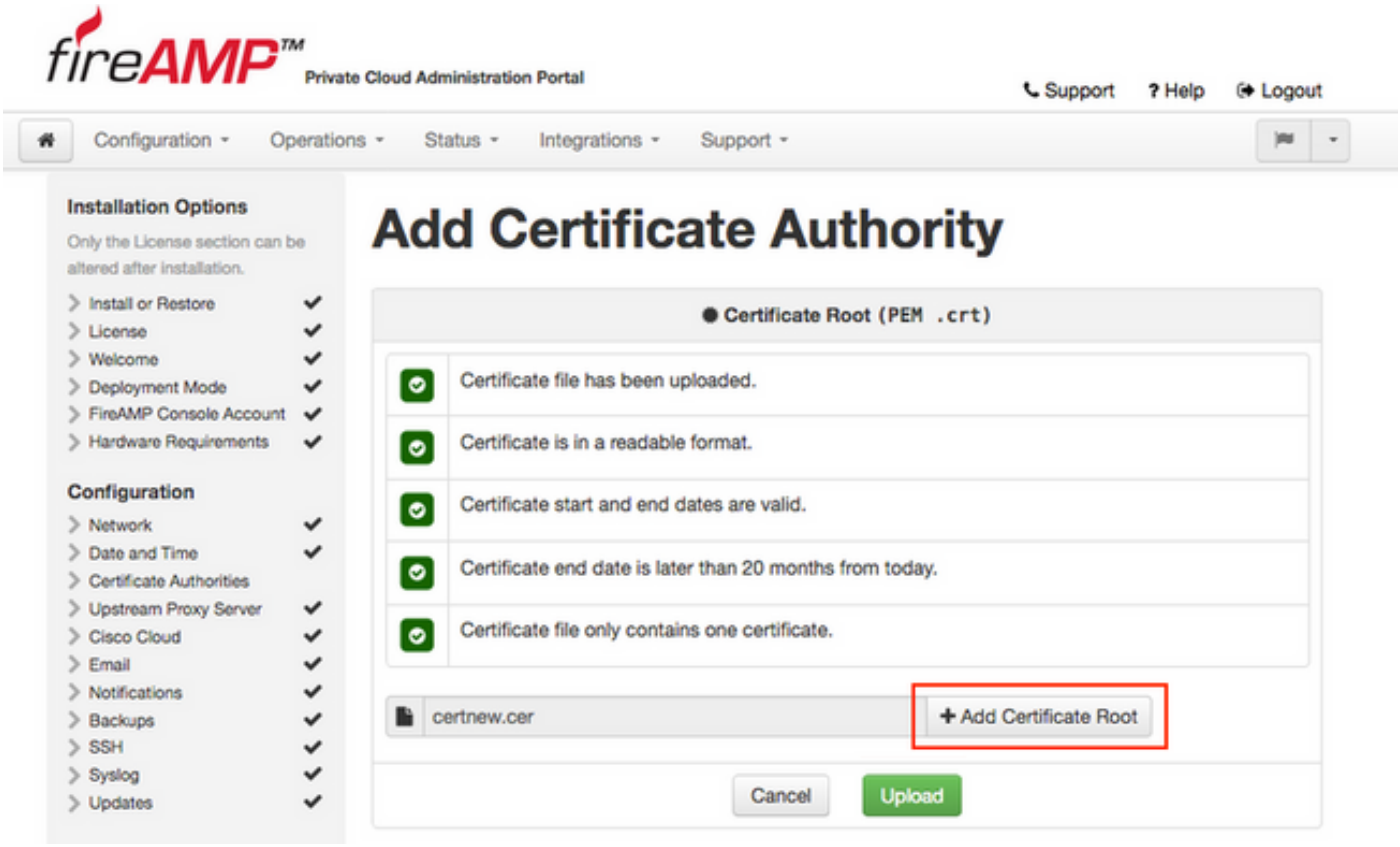
Étape 1. Accédez à la section **Configuration** -> **Autorités de certification** du panneau **Options**

d'installation. Cliquez sur le bouton **Ajouter une autorité de certification**, comme illustré dans l'image.

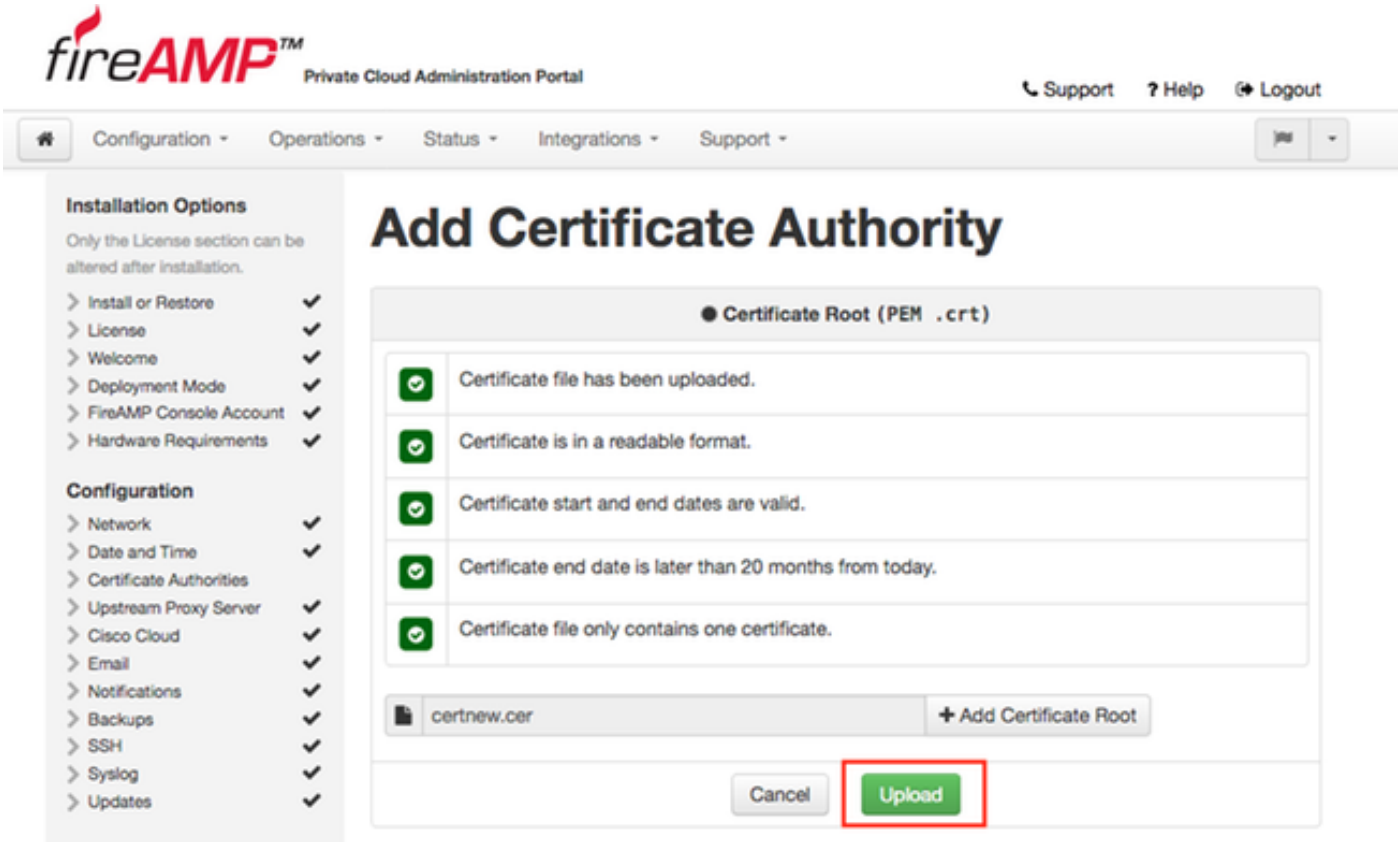


Étape 2. Cliquez sur **Ajouter la racine du certificat,** comme illustré dans l'image, pour télécharger le certificat. Toutes les conditions répertoriées doivent être remplies pour que le cloud privé virtuel accepte le certificat.

> **Note**: Au cours de la procédure de mise à niveau, vous devez ajouter un **certificat racine** utilisé pour signer le certificat de service **Authentification**, expliqué dans la section suivante.



Étape 3. Une fois le certificat mis à jour, cliquez sur le bouton **Upload**, comme illustré dans l'image, pour télécharger le certificat.



Si vous utilisez une autorité de certification subordonnée pour signer des certificats de service, téléchargez-les également dans cette section.

Attention : Même si vous générez un certificat auto-signé pour le service d'authentification,

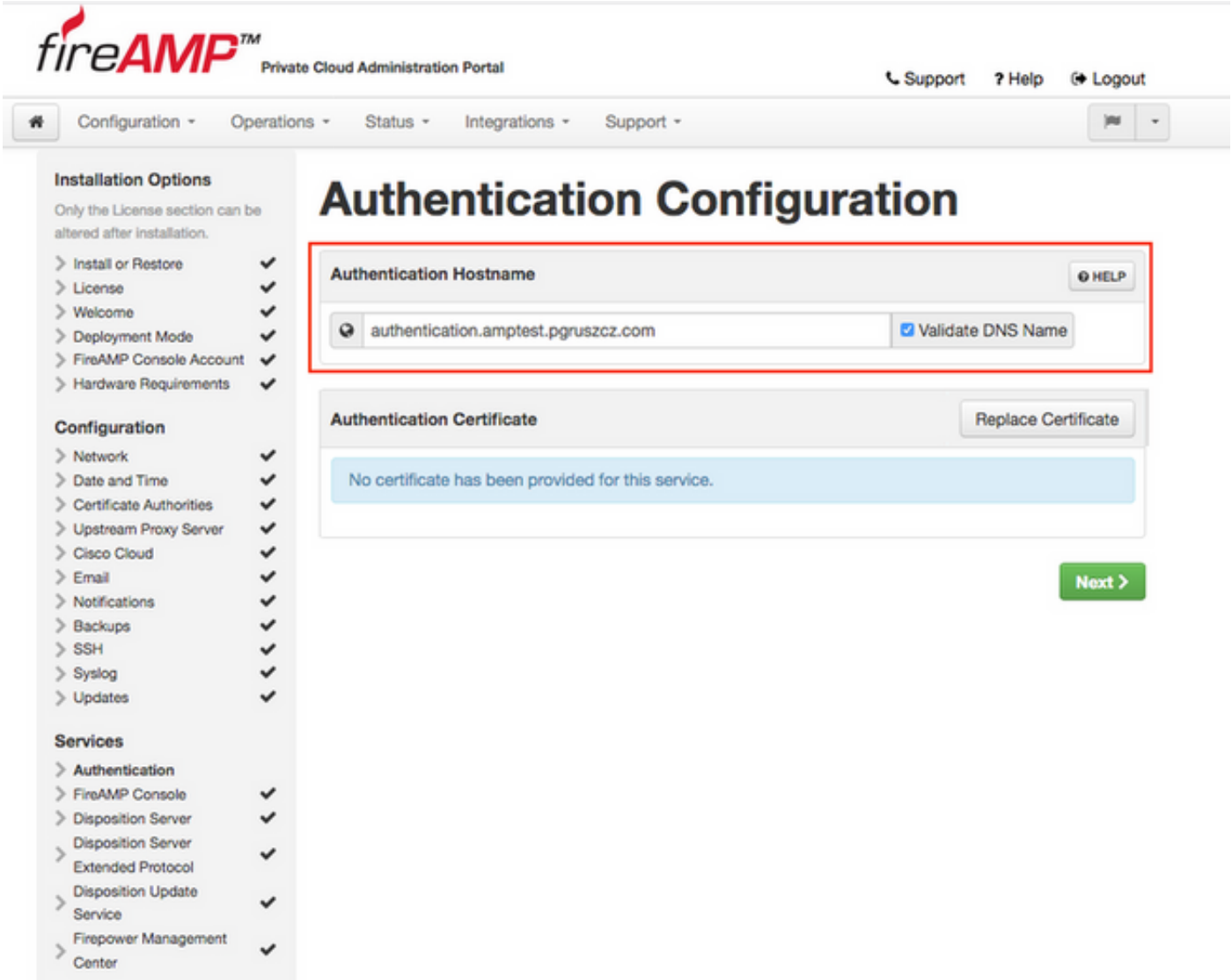
assurez-vous qu'il est chargé dans la section Autorité de certification avant d'aller aux étapes suivantes.

6. Service d'authentification

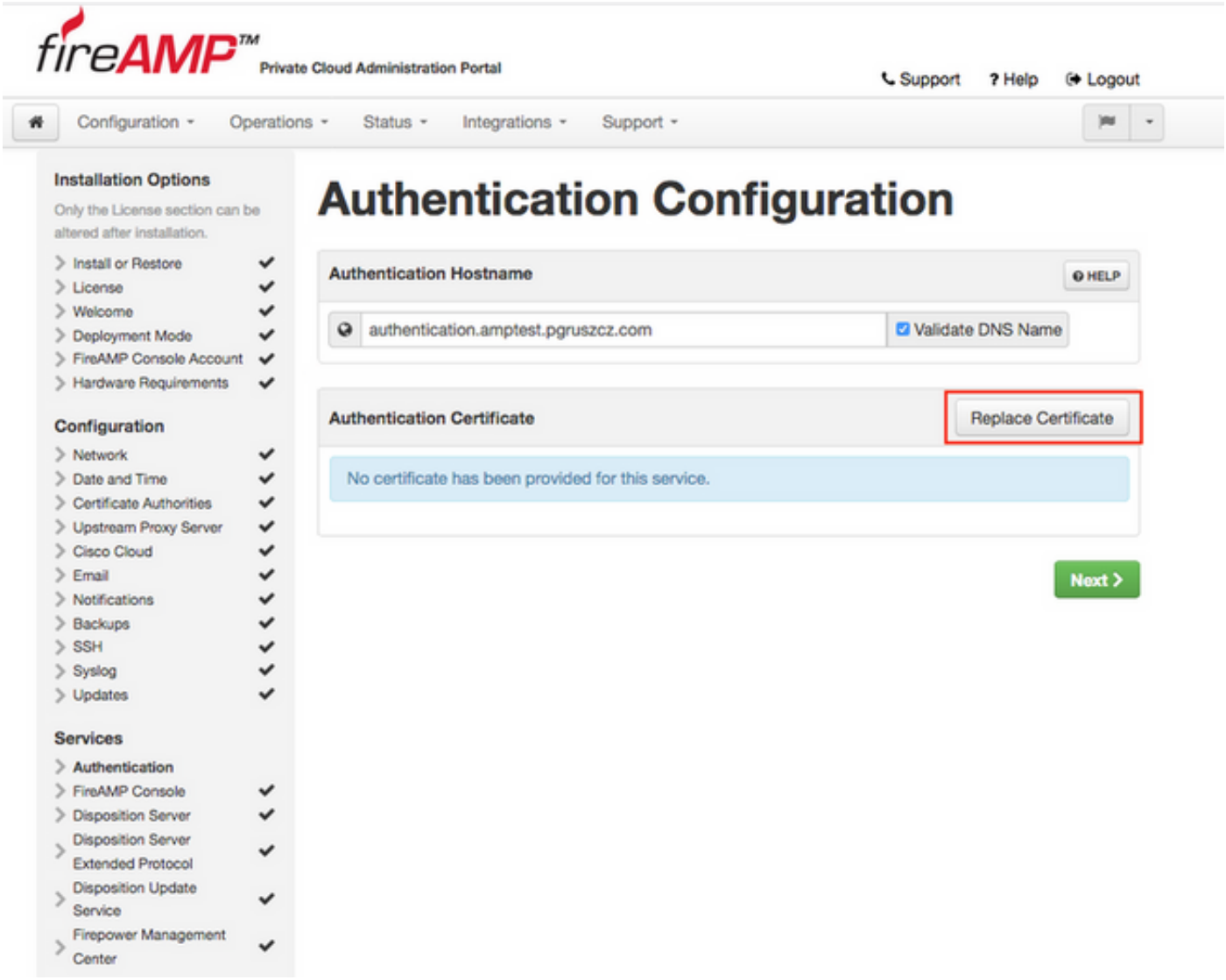
Le deuxième composant ajouté dans la version 3.0.1 et non importé de la sauvegarde est **Authentification** sous la section Services.

Le service d'**authentification** sera utilisé dans les versions futures du cloud privé pour gérer les demandes d'authentification des utilisateurs. Il est ajouté dans la version 3.0.1 pour une compatibilité future.

Étape 1. Accédez à la section **Services** -> **Authentification** du panneau **Options d'installation**. Entrez un **nom d'hôte d'authentification** unique, l'entrée DNS spécifiée dans la section hostname doit être correctement configurée sur le serveur DNS et pointe vers l'adresse IP de l'interface de la console de cloud privé virtuel.

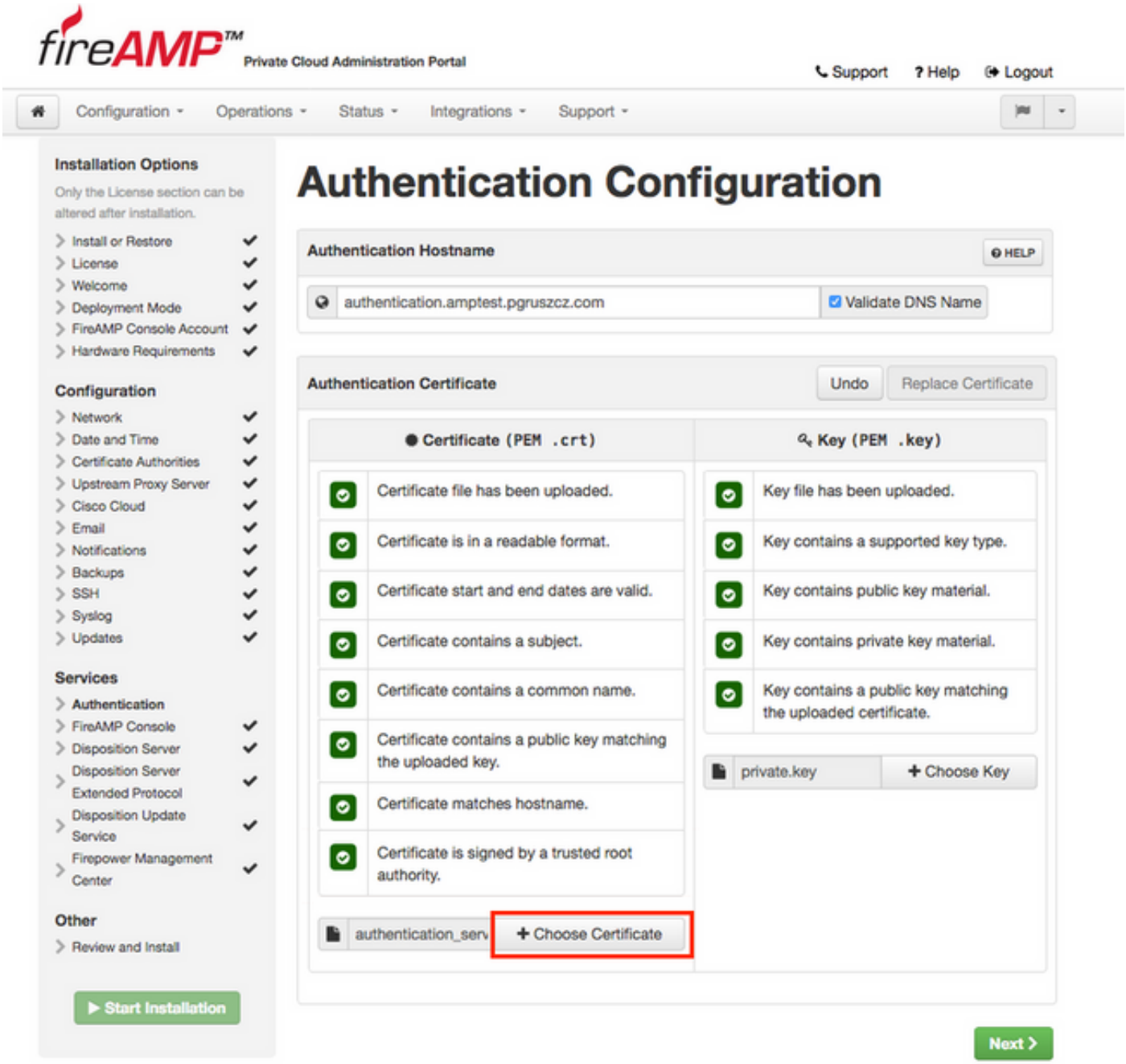


Étape 2. Une fois le nom d'hôte spécifié et résolvable, cliquez sur le bouton **Remplacer le certificat**, comme indiqué dans l'image.

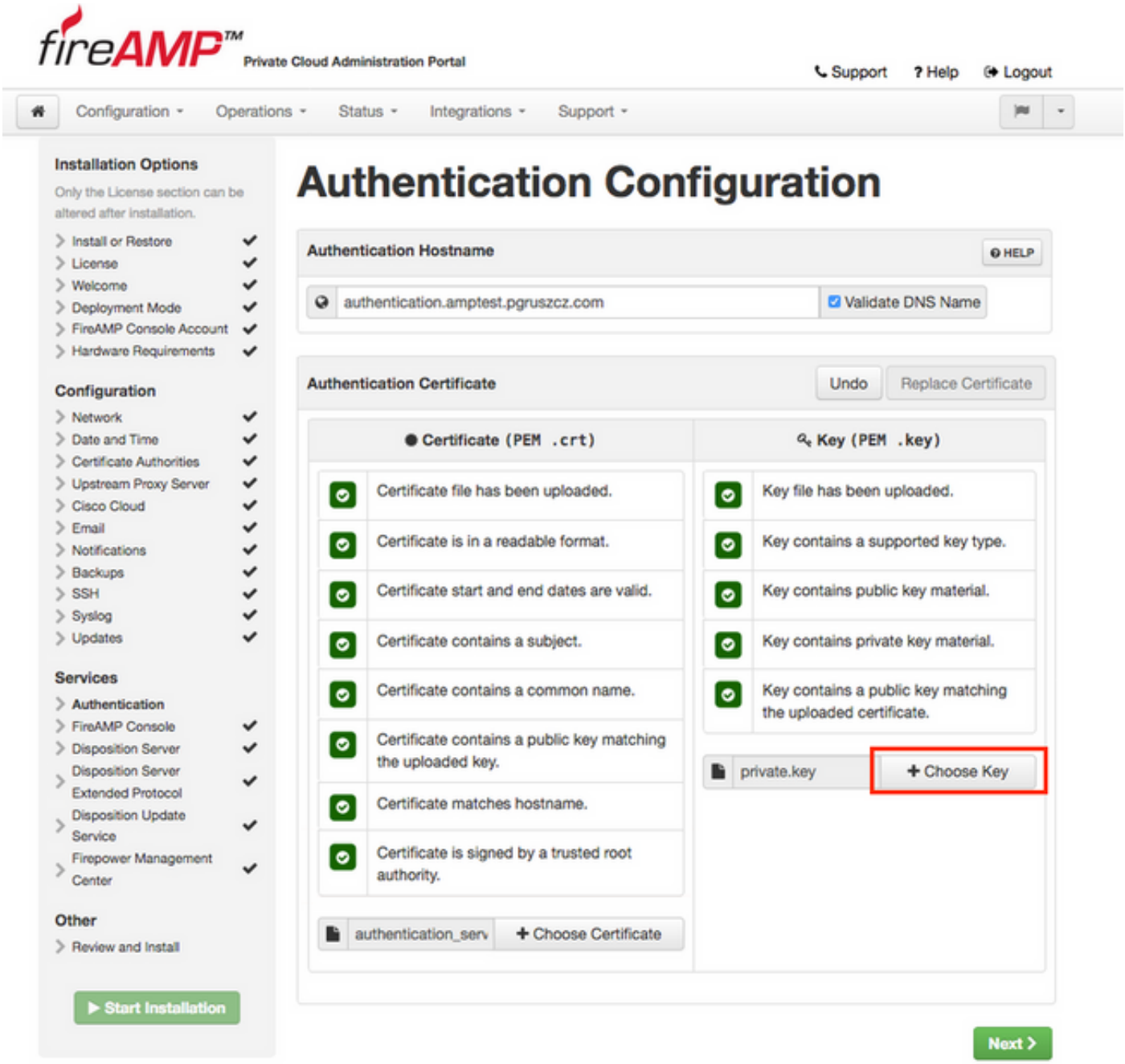


Note: Si vous avez besoin d'aide pour la génération de certificats, visitez l'article : [Comment générer et ajouter des certificats requis pour l'installation d'AMP VPC 3.x à partir de] pour plus d'informations sur la configuration matérielle requise.

Étape 3. Cliquez sur le bouton **Choisir le certificat** pour télécharger le certificat du service d'authentification, comme indiqué dans l'image.



Étape 4. L'étape suivante consiste à télécharger le fichier de clé privée pour le certificat. Pour l'ajouter, cliquez sur le bouton **Choisir une clé**.



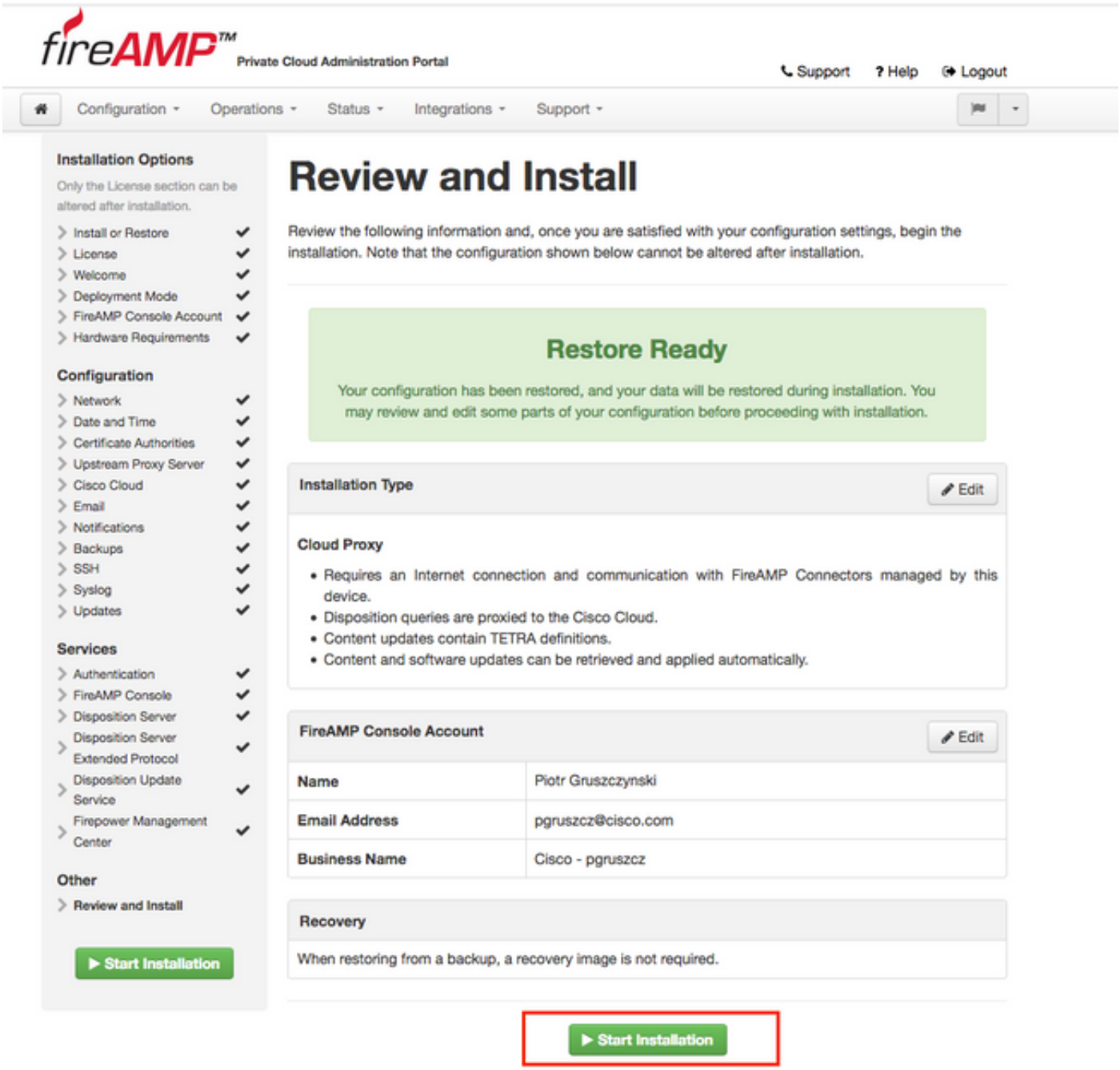
Étape 5. Vous devez vous assurer que toutes les conditions requises sont remplies avant de passer à l'étape suivante. Les conditions mises en évidence sont remplies si le certificat racine utilisé pour signer le service **d'authentification** est correctement placé dans le magasin **des autorités de certification**.

> **Attention** : Vous ne pouvez modifier les noms d'hôte de tous les autres services qu'à ce stade. Une fois l'installation terminée, le nom d'hôte des services ne peut pas être modifié. Plus tard, vous ne pourrez modifier que les certificats. Vous devez vous assurer de comprendre le risque d'une telle opération. Si vous modifiez les noms d'hôte des services utilisés par les connecteurs ou AMP pour les périphériques réseau, ils peuvent rencontrer des problèmes pour communiquer avec le cloud une fois la mise à niveau terminée.

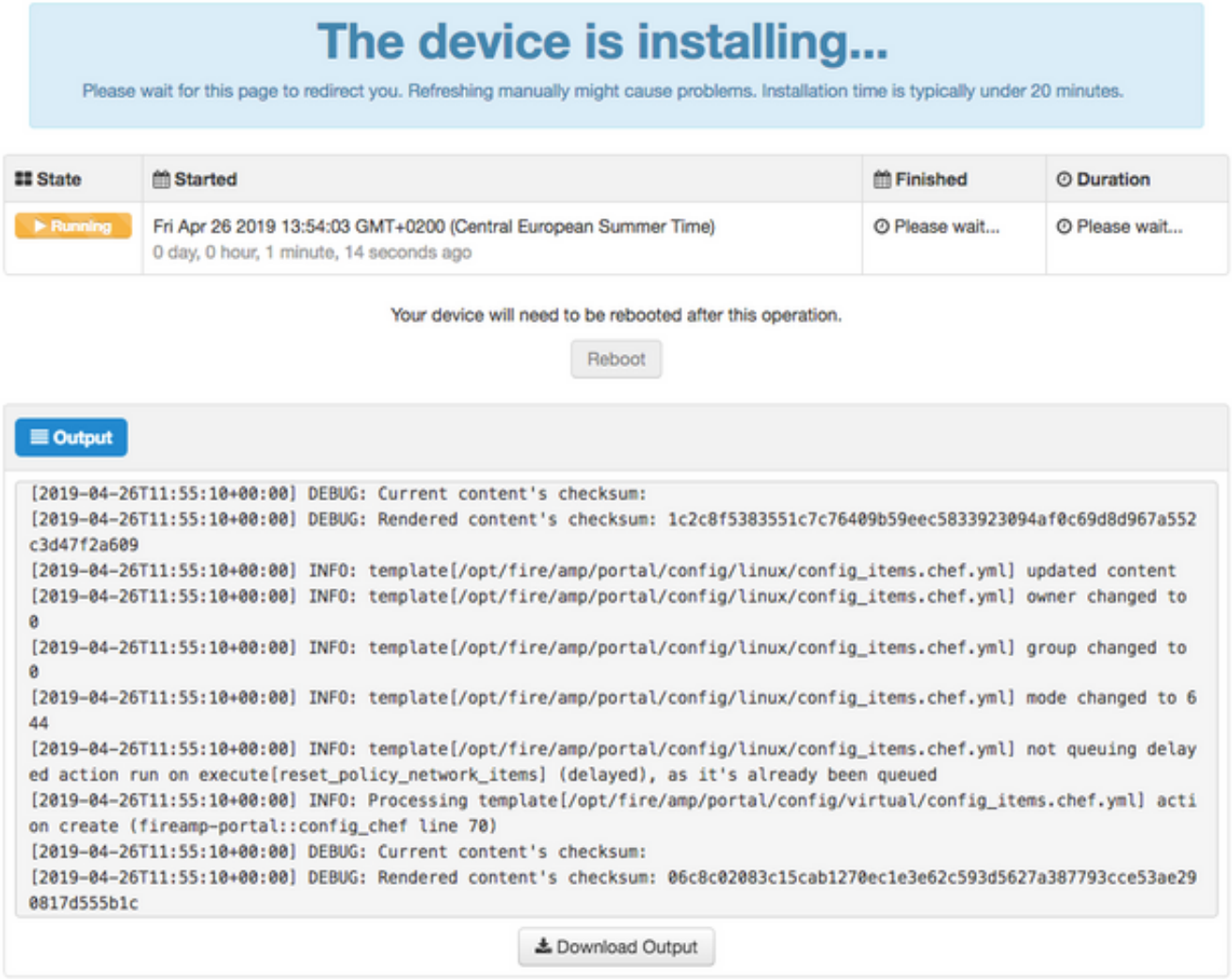
7. Installation

Étape 1. Une fois chaque section terminée et marquée comme valide, vous commencez

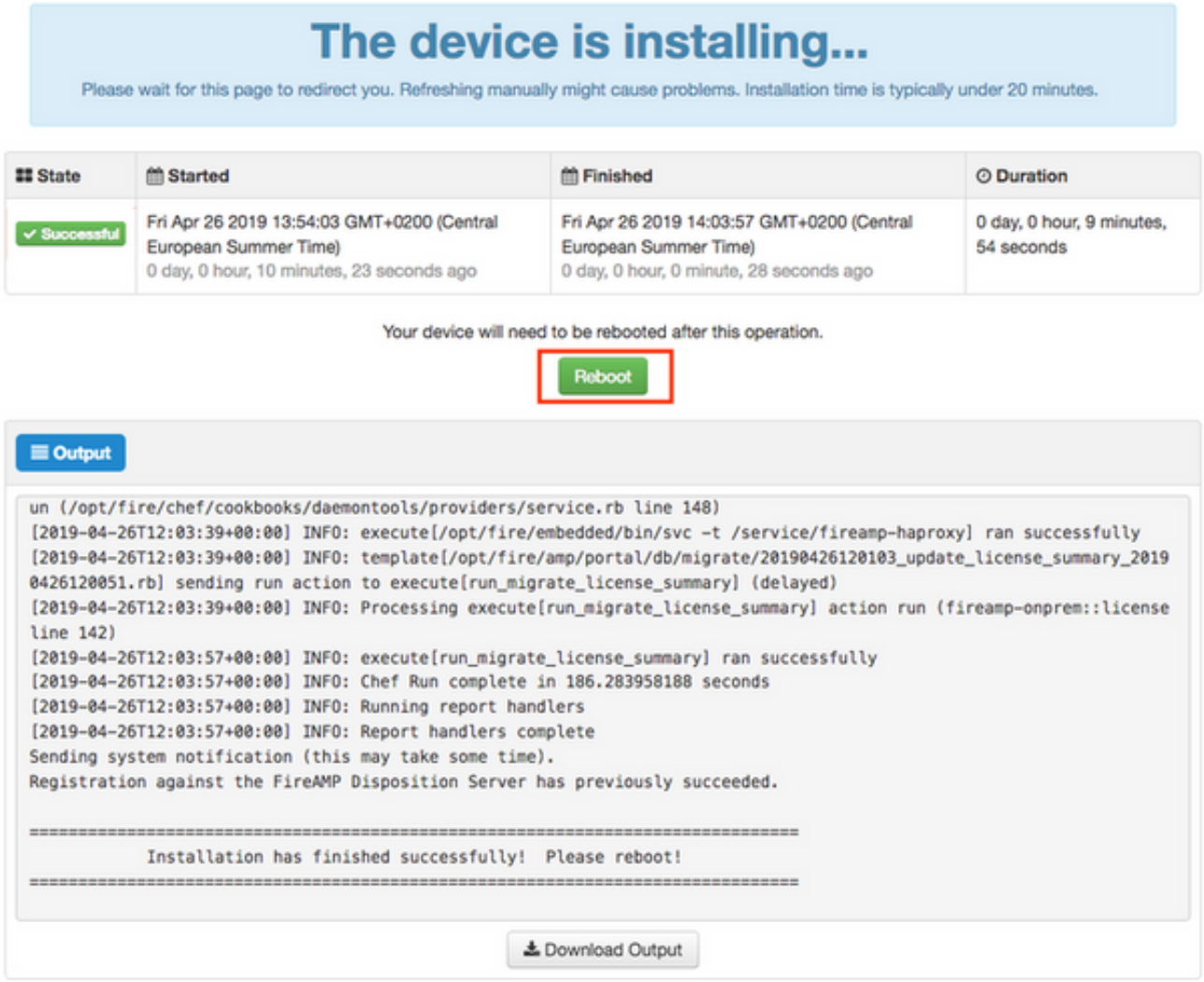
l'installation. Accédez à la section **Vérifier et installer** et cliquez sur le bouton **Démarrer l'installation**, comme illustré dans l'image.



Étape 2. Le portail Administrateur vous présente l'état actuel, la date de début et les journaux. Si vous rencontrez des erreurs ou des problèmes nécessitant une assistance, collectez les journaux en cliquant sur le bouton **Télécharger la sortie**, comme indiqué dans l'image, et associez-les au cas TAC.



Étape 3. Une fois l'installation terminée, vous devez redémarrer le périphérique pour terminer le processus. Cliquez sur le bouton **Reboot** pour poursuivre la procédure de redémarrage, comme illustré dans l'image.



Étape 4. Après la procédure de redémarrage, vous pouvez vous connecter au portail **Administrateur** et au portail **Console**. La procédure de mise à niveau est terminée.

8. Valider les contrôles de mise à niveau

Une fois le périphérique redémarré, assurez-vous que la restauration a été effectuée avec succès :

Étape 1. Vérifiez si les connecteurs peuvent communiquer avec l'appliance virtuelle 3.0.1 récemment installée.

Étape 2. Assurez-vous que l'objet Events, Device Trajectory et Computers est correctement restauré et présenté dans le portail de la console.

Étape 3. Si vous disposez d'AMP pour les intégrations réseau telles que FMC, ESA, WSA s'assure qu'ils peuvent communiquer avec le serveur de distribution de fichiers.

Étape 4. Recherchez les mises à jour de contenu/logiciel (Opérations -> Mise à jour du périphérique) et poursuivez l'installation de ces mises à jour.

Il est fortement conseillé d'effectuer des tests pour garantir une mise à niveau réussie.

Modifications apportées au cloud privé virtuel 3.0.1

1. Connecteur Windows version 6.1.7

Private Cloud 3.0.1 est livré avec la prise en charge de la version 6.1.7 du connecteur Windows. Vous pouvez trouver la documentation à son sujet sous le lien : Notes de version pour la version 6.1.7

> **Attention** : Si vous avez apporté des modifications aux certificats, assurez-vous qu'avant une mise à niveau ou une installation vers la version 6.1.7 du Connecteur Windows, les certificats utilisés pour les services de cloud privé sont approuvés sur le terminal lui-même. La confiance doit être au niveau de la machine, pas de l'utilisateur. Si cette condition n'est pas remplie, les connecteurs ne font pas confiance au certificat présenté par le cloud privé qui les maintient dans un état déconnecté.

2. Autorités de certification et service d'authentification

Les modifications ont été décrites en détail dans le guide de l'utilisateur de la version 3.0 : Guide d'utilisation du cloud privé.

Les autorités de certification vous permettent de gérer les certificats racine pour vos services si vous voulez utiliser une autorité de certificat personnalisée. Vous pouvez télécharger ou supprimer votre certificat racine si nécessaire.

Le service d'**authentification** sera utilisé dans les versions futures du cloud privé pour gérer les demandes d'authentification des utilisateurs. Il est ajouté dans la version 3.0.1 pour une compatibilité future.